REMARKS

The undersigned thanks examiner Hadi Armouche and his supervisor Mr. Gilberto Barron for the telephone interview held August 10, 2009. The agenda for the telephone interview had been faxed to the examiner on August 3, and a copy is reproduced below.

With regard to items 1-3 of the agenda, an agreement was reached that the objections to the claims in paragraphs 11-13 of the office action would be withdrawn.

With regard to item 4 of the agenda, the examiner stated that claims 152, 153 were rejected for the same reasons as claim 151; claim 203 was rejected for the same reasons as given in the office action paragraph 16; and claim 231 was rejected for the same reasons as claim 3.

An agreement was reached that claims 10, 15, 17 would be allowable if re-written as independent. As indicated in the agenda items 14-16, there are other claims believed to be allowable for similar reasons, and more particularly claims 193, 211, 198, 200. A confirmation is respectfully requested that these claims would also be allowable.

Claims 1 and 4 were discussed with respect to the Boneh reference. The examiner stated that the recitations of different keys and key pairs were confusing, and requested to provide labels for different keys and key pairs. The claims are amended to provide such labels. Reconsideration of the section 102 rejection is respectfully requested in view of the reasons given in the agenda items 5-8, 12-13.

If a fee is required for this submission, please charge the fee or any underpayment thereof, or credit any overpayment, to deposit account 50-2257.

AGENDA FAXED TO EXAMINER ON AUGUST 3, 2009

1. Claims 172, 173, 177, 181 were objected to for referring to cancelled claims, and are amended as suggested by the examiner.

2. Claim 137 was objected to, and is canceled.

3. Paragraph 13 of the office action states that claim 184 is a substantial duplicate of claim 1. This is respectfully traversed. Claim 1 recites a "method comprising

encrypting", and claim 184 recites a "method comprising decrypting". Both claims 1 and 184 are directed to operating an encryption scheme which provides for both encryption and decryption. Claim 1 would be infringed by operating the cryptosystem to perform encryption regardless of whether or not decryption is performed. Claim 184 would be infringed by a party performing decryption regardless of whether or not the party performs encryption. The claims are therefore different in scope.

4. Per the office action paragraph 15, claims 1 and 18 were rejected under 35 U.S.C. 102(e) over U.S. patent no. 7,113,594 to Boneh et al. The office action also discusses the remaining claims as anticipated by Boneh except for claims 152, 153, 203, 231. Confirmation is respectfully requested that claim 203 is allowed and claims 152, 153, 231 would be allowed if re-written in independent form.

5. Claim 1 recites two public key/private key pairs: (i) recipient public and private keys, and (ii) recipient encryption and decryption keys. As explained in the applicant's amendment filed 4 March 2009, at pages 36-38, use of two pairs of public/private keys has certain advantages in some embodiments, and Boneh teaches at most one such pair consisting of a public key ID and a private key d_{ID}.

The office action asserts in paragraph 16 that Boneh teaches both of the pairs of claim 1. However, the office action does not identify which elements of Boneh correspond to the applicant's encryption key, decryption key, public key and private key. If the rejection is maintained, the examiner is respectfully requested to identify Boneh's elements for each of the applicant's four keys recited in claim 1.

6. It appears from the office action paragraph 16 that maybe the examiner read the applicant's encryption and decryption keys on Boneh's public key ID and private key d_{ID}. In particular, the office action states that Boneh's col. 2 lines 48-55 teach that the recipient encryption key is generated from information comprising the identity of the recipient. Boneh's column 9, lines 29-33 teach a public key ID, also called "a public identifier ID for the intended receiver" (column 6, lines 26-28). A confirmation is respectfully requested that the examiner reads the applicant's encryption and decryption keys on Boneh's public key ID and private key d_{ID}.

7. Claim 4 further refers to the recipient public key, and the office action paragraph 19 states that the public key is disclosed in Boneh's column 2 lines 62-65. Boneh's column 2 lines 62-65 refer to an encryption key (assumedly ID, see paragraph 6 hereinabove) and a "message key". As described in Boneh's abstract however, the message key is secret and thus is not public as recited in claim 4.

8. There is an additional reason why the rejection of claim 4 is in error even assuming that Boneh's message key corresponded to the public key of claims 1 and 4. More particularly, claim 4 recites that "the recipient encryption key is generated from information comprising the recipient public key". According to Boneh's passage cited by the examiner (column 2 lines 62-65), the "message key is generated from the encryption key". This is the opposite of claim 4, and hence does not anticipate claim 4.

Similar reasons apply to claim 5.

9. Claim 9 and its dependent claim 10 recite:

the recipient decryption key has a value $S=s_c P_B$, where $P_B=H_1(\mathrm{Inf_B})$,

where $\mathrm{Inf_B}$ comprises the recipient public key.

Boneh's decryption key $d_{ID}=sQ_{ID}$ where $Q_{ID}=H_1(\mathrm{ID})$. See column 15 lines 40-44 and column 9 lines 29-32. Assuming for the sake of argument, as apparently done by the examiner, that:

- the applicant's decryption key S corresponds to Boneh's d_{ID},

- the applicant's $\mathrm{Inf_B}$ corresponds to Boneh's encryption key ID, and

- the applicant's public key corresponds to Boneh's message key,

there is no teaching in Boneh that his ID comprises the message key (the "public key") as recited in claim 10.

10. Claim 15 recites a ciphertext C as follows:

$C = [rP, M \oplus H_2(g^r)]$, where $g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, where PK_B is the recipient public key.

The office action (paragraph 30) refers to Boneh's column 5 line 40-column 6 line 65, but these passages do not teach or suggest the ciphertext as in claim 15. If the rejection is maintained, an explanation is requested how Boneh teaches the ciphertext of claim 15.

11. A similar request (to explain the ciphertext) is being respectfully made with respect to claim 17, reciting a ciphertext C as follows:

$$C = [rP, M \oplus H_2(g^r), E_{H_4(\sigma)}(M)], \text{ where } g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B)$$

The office action refers to Boneh's column 5 line 40-column 6 line 65 and column 24 lines 5-27, but these passages do not teach or suggest the ciphertext as in claim 17. If the rejection is maintained, an explanation is requested how Boneh teaches the ciphertext of claim 17.

12. Claims 18, 184, 203, 218, 229 are believed to be allowable for reasons similar to the reasons given above for claim 1.

13. Claims 21-22, 187-188, 206-207, 221-222, 232-233 are believed to be allowable for reasons similar to the reasons given above for claim 4.

14. Claims 193, 211 are believed to be allowable for reasons similar to the reasons given above for claim 10.

15. Claim 198 is believed to be allowable for reasons similar to the reasons given above for claim 15.

16. Claim 200 is believed to be allowable for reasons similar to the reasons given above for claim 17.

17. If a fee is required for this submission, please charge the fee or any underpayment thereof, or credit any overpayment, to deposit account 50-2257.

Any questions regarding this case can be addressed to the undersigned at the telephone number below.

Certificate of Transmission: I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office (USPTO) via the USPTO's electronic filing system on August 10, 2009.

Michael Shenker 10 August 2009

Attorney for Applicant(s) Date of Signature

Respectfully submitted,

Michael Shenker

Michael Shenker
Patent Attorney
Reg. No. 34,250
Telephone: (408) 392-9250

Law Offices Of
Haynes and Boone, LLP